HOW TO PROTECT SENSITIVE DATA AFTER AN INTERNET SECURITY BREACH

by Texas Attorney General Greg Abbott

OVER THE LAST TWO MONTHS, INTERNET security breaches at public and private institutions have compromised Texans' names, addresses and Social Security numbers. Unfortunately, online security lapses can lead to identity theft.

As law enforcement officers know, personally identifying information – including names, Social Security numbers, and driver's license numbers – in the hands of identity thieves can damage Texans' credit. An identity thief may use this sensitive information to obtain credit cards and checking accounts in their victims' names.

Texans who believe an Internet security breach may have affected them should access the Attorney General's Identity Theft Victim's Kit online at www.texasattorneygeneral.gov. The kit is designed to help victims navigate the process of protecting their credit. It includes relevant forms and agency contact information that is necessary to help restore credit and prevent further financial harm.

Texans should carefully monitor their bank statements, credit card bills and any other statements relating to recent financial transactions. They should request a copy of their credit reports and examine them carefully for signs of fraud, such as unauthorized credit accounts. Potential victims should also check to see if there have been multiple inquiries on their credit report. If a thief is attempting to open up several accounts, an inquiry will be listed on a credit report for each of those attempts. Finally, Texans should check that their Social Security number, address(es), phone number(s) and employment information are correct.

If Texans notice unusual activity on their credit statements, they should contact the fraud department of one of the three credit reporting agencies – Experian, Equifax or TransUnion – and request a fraud alert. When a person requests a fraud alert from one bureau, that company will notify the other two bureaus. The person's credit file will be flagged with a statement that says he or she may be a victim of fraud and that creditors should phone the person before extending credit. Under the Fair Credit Reporting Act (FCRA), a person can place an initial fraud alert for 90 days at a time and may cancel the fraud alert at any time.

When a person establishes a fraud alert, he or she will receive a follow-up letter from each credit bureau. Each letter explains how the person can order a free copy of his or her credit report from that credit bureau. Texans who fear their personal information has been compromised by recent Internet security breaches should take advantage of this offer and order their credit reports soon. Identity theft victims will see evidence of it on their credit reports.

ID theft victims may also consider a security freeze. Texas law authorizes individuals to place a security freeze on their credit reports if they have filed an identity theft complaint with law enforcement. A security freeze is stronger than a fraud alert because it prevents anyone from accessing a credit file until and unless the person authorizes the credit bureaus to release his or her report. (Please note that it does not affect existing accounts and includes other exceptions.) Texans should be aware that a security freeze might be inconvenient – particularly for anyone who is applying for new credit, an apartment, or employment involving a background check. For those credit checks in process, the affected individual will have to lift the freeze on their credit file. A freeze can be lifted for a certain period of time or for a specific creditor.

If credit reports indicate that a person is an ID theft victim, he or she should immediately file a police report. It is very important to complete this step because the report can be used as proof that the person is an ID theft victim.

Victims should report fraudulent accounts and erroneous information in writing to the credit bureaus and the credit issuers following the instructions provided with the credit reports. More than likely, the credit bureaus will ask for a copy of the police report.

In all communications with the credit bureaus, ID theft victims should refer to the unique identification number assigned to their credit report. They should send all communications via certified mail with return receipt requested – and be sure to save all credit reports as part of their fraud documentation.

The U.S. Department of Justice (DOJ) has the authority to prosecute identity theft at the federal level. Texans can report ID theft to federal authorities and receive additional assistance with identity theft-related issues through the Federal Trade Commission by calling (877) IDTHEFT (1-877-438-4338), or visit the agency's website at www.ftc.gov.

– May 2011